5 #TrendTips For Better File Storage Security

As more companies migrate from aging on-premises storage to the cloud, the need has increased for cloud storage to secure business' high-value objects. We take look at 5 #TrendTips to secure the valuable files and objects being stored in the cloud via services like Amazon Simple Storage Service (Amazon S3).

1. Gatekeep your buckets with access control lists

Think of your Amazon S3 buckets as exclusive subreddits, and you're the moderator with all the power to grant access.

It's up to you to set up access control lists. Keep in mind that access should be at least-privilege 99.9% of the time—only those who need access to complete their job should receive it (also known as Role Based Access Control [RBAC])

Check out these **best practice** tips from Amazon Web Services (AWS) for more info.

2. Regularly review and audit access

Security checks aren't one-and-done. Since your Amazon S3 buckets are constantly receiving new files, you need monitor the activity for any changes to your buckets.

Use **AWS IAM Access Analyzer** or **AWS CloudTrail** to regularly monitor public access to your buckets and subsequent files so you're aware of any bucket misuse ASAP.

3. Scan your files

It only takes one malware-infected file to wreak havoc on your entire enterprise environment, including your downstream workflows.

That's why files need to be scanned before being placed in your Amazon S3 buckets to detect any malware that might be lurking within.

4. Have a remediation plan in place

Scanning your files is a good first step, but you also need a game plan in case something is flagged—like setting up post-scan actions for remediation. It's even better if the remediation can be automated.

Trend Micro Cloud One™ - File Storage Security has scanning covered from start to finish. You can integrate it with Amazon Simple Notification System (SNS) so you receive alerts right away before things get out of control. Check out our **sample code** to learn more.

5. Archive your cloud data for long term storage

Similar to archiving and backing up your on-premises data, you should do the same in your cloud environment. Amazon S3 Glacier is a great place to start to safeguard your data.

Next steps

File Storage Security is just one of seven solutions making up Trend Micro Cloud One™ a SaaS-based security services platform designed for cloud builders. It is easily deployed using AWS CloudFormation templates for Amazon S3 customers to provide anti-malware inspection and protection for your downstream cloud-native workflows.

Misconfigurations can lead to wild files exploiting vulnerabilities. Trend Micro Cloud One™ - Conformity, provides auto-checks against hundreds of infrastructure configuration best practice across over 85 services from AWS and Microsoft Azure™, as well as auto-remediation for any discovered violations.

See the difference that best-in-breed cloud protection provides with a **free 30-day trial of Trend Micro Cloud One**.